CALIFORNIA HOSPITAL ASSOCIATION

Providing Leadership in Health Policy and Advocacy

Hospital Cybersecurity Planning Quick Reference Tool

The following information can be used to aid in evaluating, developing and refining an organization's cybersecurity protections, and should be reviewed with members of your information technology and emergency preparedness teams.

Background

Cyberattacks using malware or viruses can occur from internal or external sources. Common targets of health care cyberattacks include:

- Technology equipment, including computers, telephone systems, video conferencing, routers and firewalls;
- Financial and employee information;
- Clinical EHR software and equipment;
- Medical devices such as radiology equipment (CT and MRI), picture archive and communications systems (PACS), blood gas analyzers, therapeutic equipment (infusion pumps, medical lasers and LASIK surgical machines), and life support equipment (heart-lung machines, medical ventilators, extracorporeal membrane oxygenation machines and dialysis machines); and
- Building control/plant operating systems.

Checklist

- ☐ Who in executive leadership is responsible for cybersecurity?
- ☐ Does your organization have a cybersecurity policy? Is it regularly updated? Does it address potential ransomware demands?
- ☐ Has your organization completed a cybersecurity gap analysis that addresses your vulnerabilities? If so, how often is it updated? Is this reported to the Board of Directors?
- ☐ Is cybersecurity part of your organization's disaster Hazard Vulnerability Analysis?
- ☐ Who assumes responsibility and liability for outsourced information technology services?
- ☐ Do you have a cybersecurity incident response team in place that includes key functions such as IT, Legal, Finance, HR and senior business leadership? Do you practice various response scenarios using tabletop exercises and drills?
- ☐ Do you have cybersecurity insurance?
- ☐ What are the cybersecurity expectations of third party vendors, and how are these monitored and audited?
- ☐ Do you have plans to ensure continuous quality patient care and continuity of other functions in the absence of electronic information, communications or data?
- ☐ What cybersecurity education and staff training have been completed?

Resources Specific to the Health Care and Public Health Critical Infrastructure Sector

1. U.S. Food and Drug Administration Guidance to Industry: Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software: www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm077812.htm

2. Department of Homeland Security (DHS) - Cybersecurity Resources: www.dhs.gov/topic/cybersecurity

3. Health Information Management Systems Society resources: www.himss.org/library/healthcare-privacy-security

Tools to Assist with Gap Analysis and California Support Systems

1. NIST Framework to Reduce Cyber Risks to Critical Infrastructure: www.nist.gov/itl/cyberframework.cfm

2. Crosswalk between the NIST Framework and the HIPAA Security Rule: www.hhs.gov/hipaa/for-professionals/security/nist-security-hipaa-crosswalk/index.html

3. Healthcare Sector Cybersecurity Framework Implementation Guide: https://hitrustalliance.net/documents/cybersecurity/HITRUST_Healthcare_Sector_Cybersecurity_Framework_Implementation_Guide.pdf

4. SAFER Guidelines from the Office of the National Coordinator for Health Information Technology to help healthcare organizations conduct self-assessments to optimize the safety of EHRs: www.chpso.org/sites/main/files/file-attachments/safer_contingencyplanning_sg003_form_0.pdf

5. California Office of Emergency Services (Cal OES) Threat Assessment Center has developed a document on ransomware and cybersecurity; hospitals must register to obtain the document: www.calstas.org/(X(1)S(4frodry1toyalqigyvszp1iq))/default.aspx?MenuItemID=182&MenuGroup/CALSTAS+Home.html&AspxAutoDetectCookieSupport=1

6. California Hospital Disaster Preparedness planning tools and resources: www.calhospitalprepare.org/continuity-planning

Reporting and Information Sharing

1. Report cyberattacks, which are criminal acts, to local law enforcement and your fusion center/regional threat assessment center. A map and contact information for fusion centers may be found at:
   www.calstas.org/default.aspx/MenuItemID/142/MenuGroup/CALSTAS+Home.html?AspxAutoDetectCookieSupport=1

2. The National Health Information Sharing and Analysis Center (NH-SAC), a nonprofit organization responsible for public and private health care sector cybersecurity, has developed a threat intelligence platform to share information on cyber threats and vulnerabilities both in cyberspace and medical devices. This organization holds an annual summit on health care cybersecurity :
   www.nhisac.org/

3. InfraGard, a public/private partnership between the FBI and U.S. businesses that focuses on threats that could disrupt the national critical infrastructure:
   www.infragard.net/

4. Health Information Trust Alliance (HITRUST) has established a certifiable framework; distributes cyber threat briefings; and produces webinars and guides to help implement NIST's cybersecurity framework:
   www.hitrustalliance.net/